Supplemental Remarks

With regard to claim 1, Shmueli would lead one skilled in the art away from protecting the "protected software" or data, as disclosed in the present application, from being copied or duplicated or otherwise distributed by the user. Once he is authenticated by entering the authentication indicia, such as a password, the user of key 10 described in Shmueli gains access to viewing or copying software or data stored on the key 10.

Shmueli provides no indication of a protected memory component where software is not viewable or accessible by the user. Instead, Shmueli further emphasizes the absence of any such protected memory area by relying upon user authentication or encryption for the protection of data stored on the key 10: "data may be accessed from the key 10 as necessary based on the keylet and the authentication" (Shmueli, paragraph [0039]) and "Preferably, this information is encrypted and protected in the user's key 10." (Shmueli, paragraph [0063]).

Shmueli describes "a user friendly interface to run on the host computing device" (Shmueli paragraph [0005]) by which the user enters authentication indicia to gain access to data stored in key 10. In contrast, claim 1 recites authentication of the application launcher software, not the user. As stated at paragraph [0051] of present application, "the application launcher authenticates itself to the authentication agent software that resides in the protected region of the memory component." Authentication of the application launcher software, rather than of a user, helps prevent a user from accessing protected software and data stored in the protected component of the device.

Shmueli does not describe or suggest a protected memory component from which software is only accessible to be run by the application launcher software and further is not viewable or accessible by the user. Shmueli does not teach or suggest "distribution of software" with "a security mechanism that can be incorporated to protect the software that is installable or executable from the memory component by the autorun firmware." (Present application, paragraph [0045].)

Instead, Schmueli emphasize that a "user must be authenticated." Schmueli , paragraph [0011]. It will be appreciated that protecting data or software on a key 10 with the user authentication emphasized by Shmueli is an indication that the key does not include a protected memory component that is not viewable or accessible by the user.

According to the present invention, the inability to view or access protected software and data stored in a protected memory section, together with the software in the protected memory component only being accessible to be run by the application launcher software, provides a secure manner of distributing software and data without risk of it being improperly accessed, copied, duplicated, or distributed, even an authenticated user. In contrast, once having been authorized or authenticated to access the device described by Schmueli, a user gains access to all data or software stored in key 10, and protected software and data is exposed to improper viewing, copying, duplicating and distribution by the user. Applicant submits, therefore, that claim 1 is patentably distinct from the cited references.

Claim 20 has been amended to emphasize that the protected software is not viewable or accessible by the user. Claim 20 recites "a protected memory component where the protected software is stored so as not to be viewable or accessible by the user and is accessible only by the autorun software for installation or running of the protected software, thereby providing copy protection of the protected software." The rejection of claim 20 does not address this feature in the cited art. Applicant submits, therefore, that the rejection of claim 20 was improper and should be withdrawn for failure to identify in the prior art each and every feature recited in the claim. Moreover, applicant submits that claim 20 is patentably distinct from the cited art for the reasons set forth above with regard to claim 1.

Independent claim 27 recites a user operable manual switch that allows a user to select from among plural operating states that include a first state in which the autorun software is operable and a second state in which the autorun

software is not operable so that the integrated circuit flash drive memory device functions as a conventional integrated circuit flash drive memory device.

Shmueli describes a portable "key" with an authentication system that does not relate to such a switch. Kouperchaliak includes an automated, non-manual "function switch 36" that automatically switches a peripheral device between a device driver installation mode and a normal peripheral function mode according to whether the device driver string is identified on a host computer. Kouperchaliak provides no teaching or suggestion related to a user-operable switch that allows a user to select from among plural operating states that include a first state in which the autorun software is operable and a second state in which the autorun software is not operable so that the integrated circuit memory device functions as a conventional integrated circuit memory device.

Rather, the fully-automated operation of the "function switch" of Kouperchaliak relates directly to the first time or one-time installation of device drivers. The functional switch 36 is an automatic switch based on the peripheral device receiving device driver identification string, as shown in Kouperchliak at Fig 3, step 52, and described as follows.

"Upon starting the peripheral device, which generally occurs when the peripheral device is plugged in, the function switch 36 automatically switches the peripheral device over to the mass storage device emulator..... [I]f (step 52) the device related software identification string corresponding to the peripheral device of the invention is identified, then the peripheral device knows that the appropriate device-related software is installed on the computer. The mass storage device emulator 34 is disconnected (step 66) and the functional module 32 is connected." Kouperchliak, paragraph [0041].

Accordingly, Kouperchliak does not disclose or suggest "a user operable manual switch on the integrated circuit memory device." Kouperchliak further does not disclose or suggest a manual switch for user to turn on or off autorun software that is stored on the integrated circuit memory device. Applicant submits that Kouperchliak would lead one skilled in the art away from a manual switch by implementing a fully automatic function switch based on whether the peripheral device receiving the "device driver identification string".

The Examiner cites paragraph [0037] of Kouperchaliak as disclosing the user operable manual switch recited in the claim. In that passage, Kouperchaliak recites "....one or more configuration files that allow a peripheral device to be configured in different ways." Applicant notes that the configuration files of Kouperchaliak relates to software configuration files of a peripheral device, not that of a manual switch that controls the operation of the integrated circuit memory device recited in the claim. Moreover, Kouperchaliak provides no teaching or description of a manual switch that turns the autorun software on or off, as recited in the claim.

Shmueli describes a key 10 that "is preferably configured for autorun capability, which ... will allow a start-up application stored on the key 10 to start executing when the key 10 is plugged in to the USB port of the host 12. (Shmueli, paragraph [0028].) Nothing in Kouperchaliak nor Shmueli, whether taken independently or in combination, teaches or suggests any user operable manual switch, much less such a switch that turns autorun software off or on. Instead, applicant submits that Shmueli would lead one skilled in the art away from such a switch by emphasizing that the autorun capability is started upon plugging the key 10 into a host computer. Applicant submits, therefore, that claim 27 is patentably distinct from the cited references.

Independent claim 33 recites an integrated circuit wireless device that is connectable to a host computing device and includes a wireless component for enabling wireless connectivity between the host computing device and the wireless component. A memory component includes a protected memory component where the wireless application software is stored so as not to be viewable or accessible by the user. The protected memory component is accessible only by the autorun software for installation or running of the wireless application software, thereby providing copy protection of the wireless application software. Applicant submits that independent claim 33 is distinct from the cited references for reasons set forth above in regard to independent claims 1, and 20.

Moreover, neither Kouperchaliak nor Shmueli teaches or suggests a wireless component for enabling the host computing device wireless connectivity

with the wireless component. Examiner notes that Kouperchaliak did not disclose a wireless component. Shmueli discloses that key 10 may be wireless, and key 10 is capable of communicating wirelessly with the host computer.

> "The smart card 10B may be a contact-based or a contactless (wireless) smart card 10B capable of interacting with the host 12... FIG. 2C depicts a wireless communication device 10C, such as a transponder, capable of facilitating wireless communications with the host 12." Shmueli, paragraph [0033]

Accordingly, for key 10 of Shmueli to communicate wirelessly with the host, the host must first be wireless-enabled. Moreover, any wireless component on key 10 operates on key 10, and cannot operate on the host computing device. Shumeli provides no teaching or suggestion that key 10 enables wireless connectivity in the host computing device. In fact, Shmueli would lead one skilled in the art away from a wireless component in key 10 for enabling the host computing device wireless connectivity with the wireless component in key 10. Similarly, Shumeli would further lead one skilled in the art away from a memory component in key 10 for storing wireless application software operable on the host computing device.

By suggesting that key 10 may implement a discovery protocol such as Bluetooth to communicate wirelessly with the host, Shumeli further emphasizes that the host would need to be wireless-enabled before it can communicate with the key 10.

> "Whereas a physical connection with a key 10 may implement the Windows plug-and-play interface, a wireless device 10C may incorporate an automatic detection or sensing technology, such as the discovery process used by Bluetooth, which is well documented and available to those skilled in the art." Shmueli, paragraph [0033]

Applicant notes that it is well known by persons skilled in the art that Bluetooth wireless protocol and its discovery profile do not include autorun functionality. It is also well known to one skilled in the art that a Bluetooth device cannot discover another device that is not also Bluetooth enabled. As a result, key 10 cannot automatically detect or wirelessly discover a (e.g. Bluetooth) host

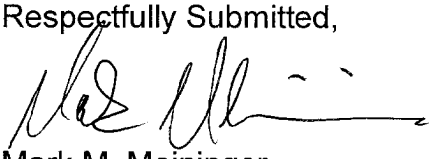
computing device unless it first Bluetooth enabled. Therefore, key 10 could not enable the host computing device with wireless connectivity with the wireless component in key 10.

Independent claim 33 further recites a memory component that includes a protected memory component where the wireless application software is stored. The protected memory component is not viewable or accessible by the user and is accessible only by the autorun software for installation or running of the wireless application software, thereby providing copy protection of the wireless application software. Applicant submits that claim 33 is patentably distinct from the cited art for the same reasons set forth above with regard to claim 1, 20.

Applicant believes the application is in condition for allowance and respectfully requests the same.

IPSOLON LLP
111 SW COLUMBIA #710
PORTLAND, OREGON 97201
TEL. (503) 249-7066
FAX (503) 249-7068

Respectfully Submitted,



Mark M. Meininger
Registration No. 32,428